DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Systems Security Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Information Security Certification and Accreditation (C&A) Methodology

Version 1.0
May 12, 2005

TABLE OF CONTENTS

1. INTRODUCTION

The CMS Certification and Accreditation (C&A) Methodology forms the foundation for an enterprise C&A program that complies with legislative requirements set forth in the Federal Information Security Management Act (FISMA) and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 (Second Draft), *Guide for the Security Certification and Accreditation of Federal Information Systems*. Section 2 provides an executive level description of the CMS C&A program, and Section 3 divides the C&A process into six distinct phases. Section 4 presents an approach for implementing and managing C&A within the CMS environment, and Section 5 provides guidance for implementing an accelerated C&A process.

2. EXECUTIVE SUMMARY

Federal law requires CMS to implement a risk-based program for cost-effective information security (IS). This requirement reinforces CMS in its efforts to protect the business processes supported by information technology platforms. All business processes operate with some level of risk, and one of the most effective ways to protect these business processes is through the implementation of effective internal security controls, risk evaluation, and risk management. To manage a risk-based IS program, CMS must assign responsibility for security; conduct Risk Assessments (RA); develop System Security Plans (SSP); review system security controls to validate that safeguards are appropriate; identify vulnerabilities and risk resulting from system implementation; authorize, in writing by the Chief Information Officer (CIO), the operation of an information system prior to full implementation and whenever significant changes in the system are affected. These processes form the foundation for the CMS Certification and Accreditation (C&A) Program, which is a critical component of the entire CMS System Development Life-Cycle (SDLC).

Through the C&A process, the CMS CIO formally authorizes the operation of an information system in a defined technical, physical, and organizational environment. The Security Certification process involves an assessment by CMS System Owners of the risks in their respective systems, and requires System Owners to identify and implement appropriate controls, and to provide sufficient information for the CIO to make informed, risk-based accreditation decisions. The Security Accreditation process requires that the CMS CIO explicitly accepts or rejects the risk associated with an information system prior to system operation, and periodically thereafter. This ensures that CMS management devotes appropriate attention and resources to IS, and that a management official is accountable for the operation of any system that creates an unreasonable risk to CMS operations, assets, or personnel.

Security certification is the comprehensive evaluation by the System Owner of the management, operational, and technical security controls implemented for an information system to ensure compliance with security requirements documented in the Federal Information Systems Controls Audit Manual (FISCAM), the CMS Information Security (IS) Acceptable Risk Safeguards (ARS), and all other standards documented within the CMS Information Security Handbook. The certification evaluation includes review of the Business RA, IS RA, SSP, other SDLC system documentation, and other findings from past assessments, reviews and/or audits, as well as technical testing and analysis. The technical certification assessment, called the System Test and Evaluation (ST&E) process, is the execution of test procedures and techniques designed to evaluate the effectiveness of security controls in a particular environment, and to identify vulnerabilities in an information system after the implementation of safeguards.

The results of the certification evaluation, together with a review of any other independent audits, reviews or assessments are documented within the ST&E report, which is delivered to the System Owner. The recommendations provided by the CMS C&A Evaluator in the ST&E report form the basis for development of a Corrective Action Plan (CAP), and are used to strengthen internal controls. The SSP and IS RA are then updated based upon improvements and changes made to system through completion of corrective actions. The output of the Security

Certification process is the Security Certification Package, which includes the Certification Form, Business RA, IS RA, SSP, CAP, and ST&E report. In addition, the CMS C&A Evaluator provides an accreditation decision recommendation to the CMS CIO or the Designated Approval Authority (CIO/DAA). The entire package is then delivered to the CMS CIO/DAA for an accreditation decision.

Security accreditation is CMS' official management decision to authorize operation of an information system. To make an informed decision, the CIO/DAA must have sufficient knowledge and understanding of the current status of the security programs and security controls in place to protect the system and information processed, stored, or transmitted by the system. This is a risk-based decision, founded upon current, credible, and comprehensive documentation and test results contained in the Security Certification Package. The System Owner must ensure that the information and resources necessary to make an informed, risk-based decision on whether to authorize operation of an information system are available to the CIO/DAA.

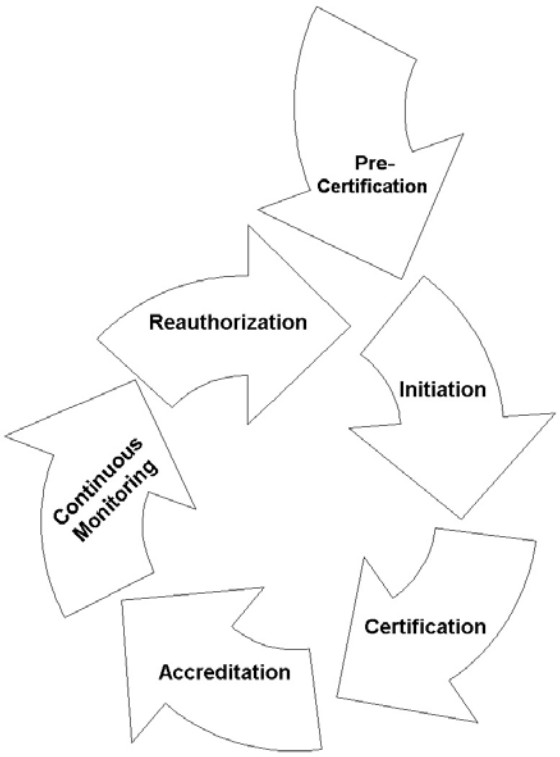
The CMS CIO/DAA must explicitly accept or reject risk to CMS operations and assets remaining after the implementation of a prescribed set of security controls. Ultimately, the CIO/DAA must strike a firm balance between authorizing the operation of information systems necessary to support completion of the CMS business mission, while ensuring that an adequate level of information security is in place. CMS must strive to implement the most effective security controls, in consideration of technical, budgetary, time, and resource limitations, while continuing to support business mission requirements.

The Security Certification and Security Accreditation processes support the FISMA legislative requirements by requiring that CMS: (1) periodically assesses the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of CMS information or information systems; (2) regularly tests and evaluates IS controls and techniques to ensure that they are implemented effectively; and, (3) periodically assesses the IS programs and practices supporting information systems.

3. CERTIFICATION AND ACCREDITATION PROCESS

The CMS C&A Process consists of six (6) distinct phases, which join together to form a continuous security management practice. Each phase has individual objectives and tasks, and completion of each successive phase depends upon the output of the preceding phase. To manage the CMS C&A process effectively and efficiently, individual tasks, responsibilities, and expectations must be defined within each phase. The C&A phases have been structured to integrate the C&A process within the existing CMS IS Program and SDLC.

The diagram to the right displays the continuous relationship between each of the six C&A phases. The following sub-sections (3.1 through 3.6) address the objectives, purpose, input, and output of each phase. Additionally, Attachment 1 to this report includes a table that demonstrates how each C&A phase and task integrates into the CMS SDLC.



In certain limited circumstances, a system may be of such great business or political significance that an immediate accreditation decision is required. An accelerated certification process is necessary to provide a quick accreditation turnaround under such circumstances. The CIO must authorize, in writing, use of the accelerated C&A process on an individual basis, and the abbreviated process must be used only under specified conditions. Refer to Section 5 of this document for guidance on implementing the accelerated C&A process.

3.1 PRE-CERTIFICATION PHASE

The objective of the Pre-Certification Phase is to integrate the C&A process documented within NIST SP 800-37 into the existing CMS IS Program, and to ensure that documentation which will serve as the foundation of subsequent C&A activities is available, adequate, and current. The Pre-Certification Phase is incorporated into the early phases of the CMS SDLC (see Attachment 1), and includes the initiation of the Business RA, the SSP, and the IS RA.

Successful completion of the Pre-Certification Phase provides sufficient information to support the transition into C&A activities. The output from this phase directly feeds the Initiation Phase of C&A process.

3.2 INITIATION PHASE

A substantial portion of the information required during this phase is initiated during the Pre-Certification Phase, and will be completed by the end of the Initiation Phase. If Pre-Certification activities were not completed, any documentation requirements from that phase must be initiated and completed during this phase. .

The objective of the Initiation Phase is to ensure that the System Owner reviews and approves the documentation developed during the Pre-Certification Phase, and that the residual risk documented within the Business RA and IS RA is in line with the CIO's expectations, before the CMS C&A Evaluator begins the ST&E process. If the System Owner refuses to accept the residual risk documented within the IS RA or Business RA, or the residual risk is not within the CIO's expectations for acceptable risk, there is no value in continuing with the certification evaluation. In this case, the SSP must be revised to comply with the CIO's expectations for acceptable residual risk. It is important to involve the CIO/DAA early in the C&A process, to communicate expectations and assumptions about C&A and risk acceptability, and to ensure that resources are used in the most efficient manner possible. After the System Owner accepts the residual risk, as documented in the SSP and IS RA, the Initiation Phase is complete, and the Security Certification Phase may begin.

A second objective of the Initiation Phase is to notify all parties who will be involved in the C&A process that an evaluation of the information system will be performed. This notification provides the System Owner the opportunity to prepare for the ST&E review, and enables the CMS C&A Evaluator to request documentation and resources that will be required in order to complete the testing and evaluation.

3.3 SECURITY CERTIFICATION PHASE

The objective of the Security Certification Phase is to ensure that management, operational, and technical security controls are sufficient to protect, at an adequate level, the confidentiality, integrity, and availability (CIA) of CMS information and information systems. The determination of whether internal security controls are sufficient and effective is made through independent testing and evaluation of the information system environment. The ST&E process is designed to identify and reveal the actual vulnerabilities remaining in the information system after internal controls have been implemented. Further, the ST&E reporting process not only documents the risk resulting from the vulnerability findings, but also provides detailed suggestions for corrective actions that will reduce or eliminate each vulnerability.

Security certification activities shall be commensurate with the System Security Level of the system. Compromise of a High System Security Level information system may result in the complete loss of mission capability for an extended period or in the loss of major assets or resources and could pose a threat to human life. Therefore, a High System Security Level information system requires more extensive testing and evaluation of internal security controls to verify that such controls are effective in preventing unauthorized access or service disruption. A large resource commitment is necessary to support a thorough certification assessment. Conversely, fewer resources shall be dedicated to certification of a Low System Security Level information system, because less harm would result from a compromise. To utilize available resources in the most efficient and valuable manner, the scope of certification activities shall be

dependent upon the System Security Level of the system, the size and complexity of the system, and the extent of the C&A review. For further guidance on scoping certification activities based upon the System Security Level, refer to the CMS C&A Procedure, Appendix B.

Following completion of this phase, information sufficient for the System Owner to determine the actual residual risk to CMS operations and assets will be available and current. This information will feed the Security Accreditation Phase to ensure that the CIO/DAA has adequate information to render an informed security accreditation decision for the information system.

3.4 SECURITY ACCREDITATION PHASE

The objective of the Security Accreditation Phase is to ensure that the actual residual risk to CMS operations or assets is acceptable to the CMS CIO/DAA. The level of acceptability of the residual risk shall be the basis for the security accreditation decision. Accreditation of an information system requires the CIO/DAA to explicitly authorize operation of the system in a particular environment, and that the CIO/DAA is accountable for any harm that that may result from such operation.

Following completion of this phase, the System Owner will have either:

1. Full authorization to operate the information system;
2. An interim approval to operate the information system under specific terms and conditions; or
3. Denial of authorization to operate the information system.

3.5 CONTINUOUS MONITORING PHASE

The Continuous Monitoring Phase ensures that C&A is not a static process within CMS. The objective of the Continuous Monitoring Phase is to provide, on an on-going basis, oversight and monitoring of the internal controls implemented for an information system, and to inform the CIO/DAA of any major changes to the information system that may impact security. To ensure that an information system authorized for use in a particular environment continues to function at an acceptable level of risk, strict configuration management and change control practices must be followed. Further, regular assessment and validation of security controls is required under Federal legislation. The activities in this phase continue until the need for re-authorization occurs.

3.6 RE-AUTHORIZATION PHASE

The Re-authorization Phase is designed to properly structure the continuous C&A process. The objective in this phase is to re-authorize operation of the information system at regular intervals and in the following situations:

1. Major system modification are made;
2. The system security level is increased;
3. A serious security violation occurs; or
4. The threat environment changes.

The Re-authorization Phase functions as formal transition between the Continuous Monitoring Phase and the Initiation Phase. During Re-authorization, the Pre-Certification Phase is bypassed and C&A activities begin in the Initiation Phase.

4. IMPLEMENTATION APPROACH

This section provides an approach for implementing the CMS C&A program, by presenting a task-based methodology for the entire C&A process. Each phase of the CMS C&A process discussed above entails one or more tasks, with a total of fifteen (15) tasks necessary to complete the full CMS C&A process. For each C&A task, there is one or more sub-tasks that must be completed. The grouping of C&A activities into a hierarchal system of phases, tasks, and sub-tasks simplifies the C&A process and facilitates milestone-based project tracking and management.

The following subsections detail the tasks and sub-tasks of the CMS C&A process. The sequence of tasks and sub-tasks presented in this section is a suggested sequence for implementing the CMS C&A process, and is not mandatory. The actual sequence of implementation of the C&A process may differ from the following approach. The flow chart included as Attachment 2 graphically displays the process flow of the C&A tasks detailed in this section.

4.1 PRE-CERTIFICATION TASKS

The Pre-Certification Phase requires that security management practices begin early in the CMS SDLC, and consists of three tasks that must be initiated before the start of any certification activities. CMS has existing processes and resource documents necessary to complete each of the three Pre-Certification tasks. The Pre-Certification tasks are as follows:

4.1.1 PERFORM BUSINESS RISK ASSESSMENT

The System Owner shall complete a Business Risk Assessment (RA) of the system and produce the Business RA Report during the Business Case Analysis or Acquisition phase of the SDLC. The end products of the Business RA shall be a determination of the current risk remaining after the implementation of security controls for the business functions; recommendations for additional or different safeguards; and a determination of the residual risk expected to remain after the implementation of the recommended safeguards. This information will be the baseline for the SSP and IS RA.

The Business RA is a precursor to the IS RA and their processes are separate and distinct.. The Business RA is an integral part of the activities performed in the first and second phases of the CMS SDLC, and focuses specifically on risk associated with business functions. The IS RA is integrated into subsequent SDLC phases and is a systematic approach for all risks associated with the information system.

The CMS Business RA Methodology shall be used to design, perform, and document the Business RA. Following completion of the Business RA, this information will be summarized in the SSP, and will serve as input to the IS RA (see Business RA and IS RA Methodology documents).

4.1.2 INITATE SYSTEM SECURITY PLAN PROCESS

The System Owner shall begin to develop an SSP for the system during the Requirements Analysis Phase of the SDLC, and complete the SSP by the end of the SDLC Development Phase. The SSP shall document the security requirements for the system, and the internal controls implemented. In addition, the SSP should include the Business RA and IS RA as attachments. The SSP will form part of the basis for the certification ST&E criteria. The CMS SSP Methodology shall be used to develop the SSP.

4.1.3 PERFORM IS RISK ASSESSMENT

The System Owner shall perform an IS RA prior to the Design Phase and produce the IS RA Report during the Development Phase of the SDLC. The IS RA must identify vulnerabilities within the system; determine the current risk remaining after the implementation of internal controls; provide recommendations for additional or improved safeguards; and determine the residual risk expected to remain after implementation of the recommended safeguards.

The CMS IS RA Methodology shall be used to design, perform, and document the IS RA. Following completion of the IS RA, the SSP should be updated to include the recommended safeguards and any updated status on their implementation.

4.2 INITIATION TASKS

To complete the C&A process successfully and in an efficient manner, proper planning and preparation must occur before the resource-intensive certification tasks begin. The Initiation Phase formally requires the completion of certain planning and preparation activities, to ensure that the system and all parties involved are ready for certification, and that all parties plan for and commit adequate resources. The Initiation Phase consists of four tasks, which ensure that:

1. Adequate and timely information is available for the CMS C&A Evaluator to understand the system environment and security requirements, at a level sufficient to design and perform a certification evaluation;
2. All parties with roles and responsibilities in the C&A process are notified of the pending certification evaluation;
3. All parties with roles and responsibilities in the C&A process have an opportunity to prepare for the certification evaluation, and allocate or obtain resources required to complete the certification evaluation; and
4. The System Owner accepts the SSP and expected level of residual risk before the CMS C&A Evaluator begins the ST&E process.

A substantial portion of the documentation necessary to complete the Initiation Phase tasks should have been initiated during the Pre-Certification Phase. This information includes the SSP, Business RA, and the IS RA. If any of this information is incomplete or outdated, it must be completed or updated before proceeding with the C&A process.

4.2.1 CERTIFICATION PREPARATION

The objective of this task is to verify that the controls described in the SSP, Business RA, and IS RA are sufficient to proceed with the certification evaluation.

Sub-task 1: Verify that the information system has been fully characterized and documented in the SSP.

Responsibility: System Owner.

Review Section 1 of the SSP to validate that all required information is included and properly documented.

Sub-task 2: Verify that the System Security Level for the information system has been correctly documented within the SSP.

Responsibility: System Owner.

The SSP shall include a designation for the system security level. Ensure that the system security level is correctly documented within the SSP. Refer to the CMS Information Security Levels for guidance.

Sub-task 3: Verify that potential threats that could exploit information system flaws or weaknesses have been identified and documented within the Business RA and IS RA.

Responsibility: System Owner.

Review the Business RA and IS RA documents to verify that potential threats have been correctly identified and documented. Refer to the CMS Business RA Methodology to determine whether potential threats to the business process have been correctly identified within the Business RA Report. Refer to the CMS Threat Identification Resource, a non-exhaustive list of possible threats, for guidance on whether additional or different threats to the information system should be included within the IS RA.

Sub-task 4: Verify that the security controls implemented for the information system have been correctly identified and documented within the SSP.

Responsibility: System Owner.

Review the Management Controls, Operational Controls, and Technical Controls sections of the SSP to verify that internal controls have been correctly identified and documented. Refer to the CMS ARS to validate that minimum standards for internal controls are satisfied. Further, refer to the CMS Information Security Handbook, FISCAM requirements, and CMS Business Partners System Security Manual to verify that appropriate security controls are implemented.

The System Owner shall identify all gaps between the documented minimum security control requirements and actual system implementation. Each gap represents a system risk that must be documented within the IS RA.

Sub-task 5: Verify that flaws or weaknesses in the information system that could be exploited by potential threats have been identified and documented within the IS RA

Responsibility: System Owner.

Verify that proper procedures have been followed to identify potential vulnerability within the information system. Further, verify that vulnerabilities documented within the SSP are consistent with industry standard and other internal CMS sources of vulnerability information.

Sub-task 6: Verify that the expected residual risk to CMS operations and assets has been determined and documented within the IS RA and Business RA.

Responsibility: System Owner.

Confirm that the Business RA and IS RA document the expected residual risk, and that the Risk Assessment and Risk Management section of the SSP addresses each High and Moderate vulnerability identified during the RA process.

4.2.2 NOTIFICATION

The objective of this task is to provide notification to all parties with roles and responsibilities within the C&A assessment of the impending assessment of information systems.

Responsibility: System Owner

Early notification of key CMS parties is critical in order to establish the C&A process as an integral part of the CMS SDLC. Further, the notification enables all parties to prepare for the upcoming tasks that will be necessary to plan, structure, and execute the certification evaluation and accreditation review.

4.2.3 RESOURCE IDENTIFICATION

Sub-task 1: Determine the level of effort required for the C&A of the information system.

Responsibility: Senior Agency Information Security Official, and CMS C&A Evaluator.

The Senior Agency Information Security Official should determine the estimated level of effort required to complete the C&A process. The level of effort shall be determined by the

System Security Level of the information system. Refer to Appendix B of the CMS C&A Procedure for further guidance on this topic.

The Senior Agency Information Security Official shall approve or modify the estimated level of effort. The CMS C&A Evaluator shall determine the actual level of effort that will be required to complete the certification evaluation, and submit this proposal to CMS. All parties shall agree to a firm level of effort estimate prior to initiating the certification evaluation.

Sub-task 2: Determine the resources required for the C&A of the information system.

Responsibility Senior Agency Information Security Official, System Owner, and CMS C&A Evaluator.

The Senior Agency Information Security Official, System Owner, and CMS C&A Evaluator shall each identify appropriate resources needed for the C&A effort. These resources shall include funding requirements and the identification of supporting organizations, personnel, and individuals with critical skills.

Sub-task 3: Prepare and authorize a C&A project plan.

Responsibility: Senior Agency Information Security Official, System Owner, and CMS C&A Evaluator.

The CMS C&A Evaluator shall develop a project plan for conducting the certification evaluation and submit the plan to CMS. The System Owner and Senior Agency Information Security Official shall approve the project plan before proceeding with the certification process.

4.2.4 SECURITY DOCUMENTATION ANALYSIS, UPDATE, AND ACCEPTANCE

The objectives of this task are to obtain an independent analysis of the Business RA, SSP and IS RA; implement additional controls to strengthen system security; update the Business RA, SSP and IS RA as required; and obtain acceptance of the SSP by the System Owner prior to execution of the certification evaluation. For greater detail on the review, update, and acceptance of the SSP, refer to the CMS System Security Plan Methodology.

Sub-task 1: Analyze the SSP and IS RA to determine if the system security controls are adequate.

Responsibility: CMS C&A Evaluator.

The CMS C&A Evaluator shall review the Business RA, SSP and IS RA to determine if the plan is complete, and to determine, based upon the ARS and other CMS information security

standards, whether the security controls implemented for the system are adequate. Based upon the results of this analysis, the CMS C&A Evaluator may recommend to the System Owner that additional security controls be implemented for the system. The recommended security controls shall comply with the CMS ARS, FISCAM requirements, and all other standards documented within the CMS Information Security Handbook.

Sub-task 2: Modify system security controls based upon the results of the independent analysis and recommendations issued by the CMS C&A Evaluator, and update the SSP and IS RA.

Responsibility: System Owner and Information System Security Officer (ISSO).

The System Owner shall review the system security controls recommended by the CMS C&A Evaluator, and implement all reasonable and appropriate security controls. The System Owner shall update the SSP to include all security controls implemented for the information system. The System Owner must also update the IS RA to include all security controls, and a revised residual risk determination.

Sub-task 3: Review the SSP and IS RA to determine if the expected residual risk to CMS operations and assets is acceptable.

Responsibility: System Owner

The System Owner shall review the Business RA, SSP and IS RA to determine if the expected residual risk complies with the CIO's expectations for acceptable risk. If the System Owner determines that the expected residual risk is not acceptable, appropriate action shall be taken to reduce system risk. The System Owner is responsible for strengthening security controls and revising the Business RA, SSP and IS RA to comply with the CIO's expectations for acceptable residual risk.

If the System Owner determines that the expected residual risk is acceptable, the Business RA, SSP and IS RA are authorized, and the System Owner agrees to proceed to the Security Certification Phase.

4.3 SECURITY CERTIFICATION TASKS

The Security Certification Phase consists of three tasks, which ensure that internal security controls are sufficient to protect the CIA of CMS information and information systems, to report the risk resulting from vulnerabilities identified during the ST&E review, and to provide detailed suggestions for developing CAPs to address each vulnerability.

4.3.1 SECURITY CONTROL VERIFICATION

The objectives of this task are to: (1) prepare for the evaluation of internal security controls; (2) evaluate the internal security controls for the information system; and, (3) document the results of the evaluation. Preparation for the ST&E process includes gathering appropriate materials and documentation, and developing ST&E techniques and procedures. After completion of the ST&E process, the CMS C&A Evaluator will be able to describe the actual vulnerabilities in the information system, and shall provide detailed corrective action recommendations to the System Owner.

Sub-task 1: Request and assemble all documentation, materials, and resources required for completion of the ST&E review.

Responsibility: Senior Agency Information Security Official and CMS C&A Evaluator.

The CMS C&A Evaluator shall develop a set of prerequisites necessary to complete the C&A review. The prerequisites document shall be delivered to the Senior Agency Information Security Official, and the System Owner shall assemble the appropriate resources requested by the CMS C&A Evaluator.

Sub-task 2: Assemble and review previous evaluation results of the security controls implemented for the information system, and determine whether previous results are suitable for reuse.

Responsibility: CMS C&A Evaluator.

The CMS C&A Evaluator shall review previous evaluation, security test results, and any outstanding findings to determine whether any previous assessment results are suitable for reuse in the current certification evaluation. Reuse of previous results may significantly increase the efficiency and cost-effectiveness of the certification process, and should be performed whenever reasonable and appropriate. Where previous results are available, and the CMS C&A Evaluator has sufficient information to determine how the test was conducted and what the actual results were, the CMS C&A Evaluator should not duplicate the effort. ST&E procedures shall be designed to evaluate only those portions of the information system for which previous results are unavailable, outdated, or considered inappropriate or inaccurate.

Sub-task 3: Develop and authorize the ST&E Rules of Engagement.

Responsibility: CMS C&A Evaluator, Senior Agency Information Security Official, and System Owner.

The CMS C&A Evaluator shall develop the ST&E Rules of Engagement that will govern the testing and evaluation activities.

The standard Rules of Engagement are included within this document as Attachment 3. The Senior Agency Information Security Official, System Owner, and the CMS C&A Evaluator must assent to the terms of the Rules of Engagement before proceeding with the certification tasks.

Sub-task 4: Develop and authorize the ST&E Work Plan.

Responsibility: CMS C&A Evaluator, Senior Agency Information Security Official, and System Owner.

The CMS C&A Evaluator shall develop the ST&E Work Plan, which will include all testing and evaluation procedures and techniques necessary to evaluate the management, operational, and technical security controls implemented to protect the information system. The ST&E Work Plan template is included within this document as Attachment 4. The Sample ST&E Work Plan is available from on Cyber Tyger web page at cms.hhs.gov/CyberTyger. The CMS C&A Evaluator shall use the sample work plan as a baseline for developing the system or site-specific ST&E Work Plan.

Test and evaluation procedures and techniques should be selected according to the management, operational, and technical controls implemented for the information system; internal controls documented within the SSP, FISCAM, CMS ARS, and all other standards documented within the CMS Information Security Handbook; the system platform and configuration; and the System Security Level. Only those test procedures and techniques relevant to the information system security controls, platform, and configuration should be selected or developed. The scope of ST&E test procedures shall be commensurate with the System Security Level, in order to use available resources efficiently. Refer to Appendix B of the CMS C&A Procedure for further guidance on tailoring the ST&E Work Plan to the System Security Level.

The Senior Agency Information Security Official, System Owner, and the CMS C&A Evaluator must agree to the test and evaluation procedures and techniques before proceeding with the certification tasks.

Sub-task 5: Perform system security test and evaluation.

Responsibility: CMS C&A Evaluator.

The CMS C&A Evaluator shall evaluate the management, operational, and technical security controls implemented to

protect the information system using the testing and evaluation techniques and procedures contained in the ST&E work plan. The CMS C&A Evaluator shall determine the effectiveness of the internal controls in a particular operational environment, and identify vulnerabilities and weaknesses remaining in the system after the implementation of security controls.

The CMS C&A Evaluator shall maintain a running list of vulnerabilities and weaknesses identified during the ST&E process, and assign appropriate personnel to document his/her findings.

Sub-task 6: Prepare the ST&E report.

Responsibility: CMS C&A Evaluator.

The CMS C&A Evaluator shall develop the ST&E report, which will include a detailed description of all procedural and technical risks identified during the ST&E process, and recommendations for reducing or eliminating each vulnerability. Attachment 5 to this document, ST&E Business Risk Template, includes the template that shall be used to document each ST&E vulnerability finding. In preparing the ST&E report, the CMS C&A Evaluator shall refer to the CMS Reporting Standard for Security Testing for guidance on formatting and developing the report.

4.3.2 SECURITY CERTIFICATION DOCUMENTATION

Sub-task 1: Provide the ST&E report to the Senior Agency Information Security Official and System Owner.

Responsibility: CMS C&A Evaluator, Senior Agency Information Security Official, and System Owner.

The CMS C&A Evaluator shall submit the ST&E report to the Senior Agency Information Security Official, who shall deliver the report to the System Owner. The System Owner may choose to complete certain corrective actions recommended by the CMS C&A Evaluator before the Security Certification Package is finalized if there are specific opportunities to reduce or eliminate vulnerabilities in the information system prior to the final security accreditation decision. The System Owner shall focus particularly on closing high-risk vulnerabilities before submitting the Security Certification Package. If corrective action is taken before the CMS C&A Evaluator issues the final report, the System Owner shall notify the CMS C&A Evaluator, who shall then update the Status section of each finding to provide evidence that certain remediation actions have been completed.

Sub-task 2: Develop the system CAP and update the SSP based upon the results of the ST&E, and any modifications to the security controls in the information system.

Responsibility: System Owner, ISSO.

The System Owner and ISSO shall collaborate to develop the system CAP. The System Owner shall update the SSP to reflect the actual state of the security controls after the security evaluation and completion of any corrective actions. At the conclusion of the Security Certification Phase, the SSP shall contain an accurate list and description of the internal security controls and a description of the actual vulnerabilities in the information system resulting from the ineffectiveness or absence of security controls. The actual vulnerabilities shall replace the expected vulnerabilities described in the original SSP.

Sub-task 3: Assemble and deliver the Security Certification Package.

Responsibility: System Owner, Senior Agency Information Security Official, and CMS C&A Evaluator.

The Security Certification Package shall contain information sufficient for the CIO/DAA to make an informed, risk-based decision to authorize or deny operation of the information system. Attachment 6 to this document includes a sample Security Certification Package cover letter that should be used as a baseline for the system-specific cover letter. Attachment 7 contains the standard CMS Security Certification Form. Attachment 8 includes a sample memorandum that should be used as a baseline for the accreditation decision recommendation.

After assembling the required information, the System Owner shall deliver the Security Certification Package to the Senior Agency Information Security Official, who shall transmit the package to the CIO/DAA using a delivery method appropriate under the circumstances. Due to the sensitive nature of the Security Certification Package, it shall be protected in both electronic and hard copy format in accordance with the CMS Information Security Policies.

4.4 SECURITY ACCREDITATION TASKS

The Security Accreditation Phase consists of two tasks, which ensure that the actual residual risk to CMS operations or assets is acceptable to the CMS CIO/DAA, and that the CIO/DAA has sufficient information to render an informed decision as to whether or not to authorize the operation of the system in a particular environment.

4.4.1 SECURITY ACCREDITATION DECISION

The objectives of this task are to evaluate the actual residual risk to CMS operations and assets, determine if the actual residual risk is acceptable, and prepare the final Security Accreditation Package. The information contained in the Security Certification Package provides the CIO/DAA sufficient information to render an informed accreditation decision, including a list of the actual vulnerabilities in the information system and a list of planned or completed corrective actions intended to reduce or eliminate each vulnerability. This information forms the basis for the determination of the final residual risk to CMS, and the acceptability of that risk.

Sub-task 1: Review the actual residual risk to CMS operations and assets based upon the confirmed vulnerabilities in the information system, and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.

Responsibility: CIO/DAA.

The CIO/DAA shall review the Security Certification Package, and assess the actual vulnerabilities identified by the CMS C&A Evaluator to determine how those vulnerabilities translate into actual risk to CMS operations and assets. The CMS C&A Evaluator, in developing the ST&E report should have performed a general translation of vulnerability into business risk, however, the CIO/DAA must utilize his/her thorough knowledge of CMS business functions, requirements, and operations to interpret the true business risk created by each vulnerability. The CIO/DAA shall determine which system vulnerabilities are of greatest concern to CMS, which are not acceptable under any circumstances, and which vulnerabilities can be tolerated without creating an unreasonable risk to CMS operations and assets.

Based upon the analysis of the business risk created by each vulnerability, the CIO/DAA shall determine the total residual risk created by operation of the information system in the proposed environment. The total residual risk shall form the basis for the security accreditation decision.

Sub-task 2: Determine if the actual residual risk to CMS operations and assets is acceptable.

Responsibility: CIO/DAA.

To determine if the actual residual risk to CMS operations and assets is acceptable, the CIO/DAA must balance CMS business mission and operational requirements with the security considerations documented within the Security Certification Package. If the CIO/DAA deems the actual residual risk to CMS operations and assets acceptable, a full authorization to operate

the information system in the proposed environment shall be issued. In this case, the system is accredited with only minimal operational restrictions or limitations, if any.

If the CIO/DAA does not deem the actual residual risk to CMS operations and assets fully acceptable, but there is a strong CMS mission-related interest to place the system into operation, an interim approval to operate may be issued. The interim approval shall be a limited authorization to operate under specific terms and conditions. The CIO/DAA may require the System Owner to complete certain corrective actions within a stated period of time, and a detailed plan of action and milestones shall be submitted by the System Owner and approved by the CIO/DAA prior to the interim approval taking effect. The information system is not accredited during the period of limited authorization to operate.

If the CIO/DAA deems the actual residual risk to CMS operations and assets unacceptable, the information system shall not be authorized for operation, and will, therefore, not be accredited.

4.4.2 SECURITY ACCREDITATION DOCUMENTATION

The objectives of this task are to prepare and submit the final Security Accreditation Package and to update the SSP with the most current information from the accreditation decision.

Sub-task 1: Prepare the final Security Accreditation Package, and transmit copies of the final Security Accreditation Package to the Senior Agency Information Security Official, System Owner, and any other CMS officials having an interest in the security or operation of the information system.

Responsibility: CIO/DAA, Senior Agency Information Security Official.

The Security Accreditation Package shall contain a security accreditation decision letter signed by the CIO/DAA and a Security Accreditation Form. Attachment 9 to this document includes a sample security accreditation decision letter, which should be used as a baseline for the system-specific accreditation decision. Attachment 10 includes the standard CMS Security Accreditation Form.

Sub-task 2: Update the SSP and CAP, if necessary, based upon the final determination of actual residual risk to CMS operations and assets.

Responsibility: System Owner and ISSO.

The System Owner shall update the SSP to reflect any changes made to the information system as a result of the Security Accreditation Phase. Any conditions set forth in the accreditation decision should also be noted in the SSP. It is expected that any changes to the SSP at this phase in the C&A process will be minimal.

4.5 CONTINUOUS MONITORING TASKS

The Continuous Monitoring Phase ensures that C&A is not a static process within CMS. The Continuous Monitoring Phase consists of three tasks that provide, on an on-going basis, oversight and monitoring of the internal controls implemented for an information system, and inform the CIO/DAA of any major changes to the information system that may impact security.

4.5.1 CONFIGURATION MANAGEMENT AND CHANGE CONTROL

Sub-task 1: Use CMS configuration management and change control policies and procedures to document proposed or actual changes to the information system.

Responsibility: System Owner, ISSO.

The System Owner shall document and record any relevant information about proposed or actual changes to the system hardware, firmware, or software, in accordance with CMS Software Quality Assurance Policy and the CMS Investment Management Policy. The System Owner shall also document any changes to the operating environment, including modifications to the physical environment.

Sub-task 2: Analyze the proposed or actual changes to the information system to determine the information security impact of such changes.

Responsibility: System Owner, ISSO, and CIO/DAA.

Prior to making any significant changes to the information system, the System Owner and ISSO shall assess the security impact of such changes. If changes have been made, the CIO/DAA may, at his/her discretion, revoke the system accreditation entirely or revoke the full accreditation and grant an interim approval.

4.5.2 ON-GOING SECURITY CONTROL VALIDATION

The objectives of this task are to select an appropriate set of internal security controls to monitor and to evaluate on a continuous basis, the effectiveness of the selected controls using industry standard validation procedures and techniques. On-going security control validation enables CMS, pro-actively, to monitor and identify potential security problems in the information system

that are not identified during the security impact assessment conducted as part of the configuration management and change controls processes.

Sub-task 1: Identify a sub-set of the security controls in the information system that should be evaluated to determine the continued effectiveness of those controls in providing appropriate protection for the system.

Responsibility: System Owner, ISSO, and Senior Agency Information Security Official.

The System Owner and ISSO shall identify and select a set of security controls to be monitored regularly. These selections shall reflect CMS IS priorities, and the importance of the information system to CMS operations. Those security controls that, if compromised, would result in the greatest harm to CMS operations and assets should be monitored. The System Security Level of the system, in accordance with the CMS Information Security Levels, shall define the scope of the on-going security control validation. For High System Security Level information systems, a greater number and breadth of security controls shall be monitored on a regular basis. Conversely, a smaller number of security controls may be monitored for Low System Security Level systems.

The Senior Agency Information Security Official shall review the set of the security controls to be monitored, and approve of each selection. The Senior Agency Information Security Official shall recommend or require certain security controls to be removed or added to the set.

Sub-task 2: Evaluate the agreed-upon set of security controls in the information system to ensure the continued effectiveness of those controls in providing appropriate protection for the system.

Responsibility: System Owner and ISSO.

Regular validation of security controls may be accomplished by performing independent or internal security reviews, self-assessments consistent with NIST SP 800-26, ST&E, penetration testing, and/or audits. Standard evaluation procedures and techniques, similar to the certification ST&E procedures and techniques, shall be employed to determine the effectiveness of the security controls. In addition, standardized evaluation procedures and techniques documented within NIST SP 800-53A shall be used where appropriate. The frequency and intensity with which such evaluations are to be performed shall be commensurate with the potential harm to CMS operations and

assets that might result from compromise of the information system. For High System Security Level information systems, the selected set of security controls shall be evaluated more frequently and more intensive procedures and techniques shall be employed. Security controls implemented to protect Low System Security Level information systems may be reviewed less often and in a less intensive manner. Refer to Section 4 of the CMS ARS for security control evaluation and validation standards.

4.5.3 STATUS REPORTING AND DOCUMENTATION

The objectives of this task are to update the SSP to reflect the most recent proposed or actual system changes and the potential security impact associated with each change, and to report the proposed or actual changes and associated security impact to the CIO/DAA.

Sub-task 1: Update the SSP based upon the documented changes to the information system and the results of the on-going security control monitoring process.

Responsibility: System Owner and ISSO.

The System Owner shall update the SSP to ensure that the plan contains the most current security-related information. During each update of the SSP, the System Security Level designation shall be re-evaluated.

Sub-task 2: Report the security status of the information system to the Senior Agency Information Security Official and CIO/DAA.

Responsibility: System Owner.

The System Owner shall prepare and submit status reports to the Senior Agency Information Security Official and CIO/DAA on a regular basis. The System Security Level of the system shall determine the frequency with which status reports must be submitted. Refer to the CMS C&A Procedures for guidance on how often status reports must be submitted.

The status reports shall serve as a basis for the Senior Agency Information Security Official and CIO/DAA to monitor the security status of the information system; the progress made to reduce or eliminate vulnerabilities; and to determine when re-authorization is necessary.

4.6 RE-AUTHORIZATION TASKS

Re-authorization is necessary to ensure that CMS information systems continue to operate at an acceptable risk level. Over the life of the information system, many changes are made that reduce the effectiveness of internal security controls, and security controls typically become

outdated and less effective as threats and vulnerabilities evolve. The objective of the re-authorization tasks is to ensure that C&A is not a one-time process, and that IS is managed throughout the life of an information system.

Sub-task 1: Determine when re-authorization is necessary, and notify the System Owner and CIO/DAA.

Responsibility: Senior Agency Information Security Official

The Senior Agency Information Security Official shall determine when re-authorization is necessary for a particular information system. The CIO/DAA shall require regular re-authorization of CMS information systems in accordance with the CMS Information Security Handbook. As a matter of practice, all information systems shall be re-authorized at least once every three (3) years, or when significant changes to the information system adversely affect system security. The following conditions also require re-authorization:

1. The system security level is increased;
2. A serious security violation occurs; or
3. The threat environment changes.

Sub-task 2: Perform system re-authorization.

Responsibility: System Owner, CIO/DAA.

After the Senior Agency Information Security Official determines that re-authorization is necessary, and notifies the CIO/DAA and System Owner of the need for re-authorization, the current system accreditation shall remain valid until the documented expiration date. If the information system is not re-authorized by this expiration date, operation of the information system is not authorized.

The re-authorization process shall begin at the Initiation Phase of the CMS C&A Methodology. Depending upon the magnitude of changes to the information system since the previous certification evaluation, the availability of evaluation results and reports, and the system risk level, the resources required for re-authorization may be substantially less than those required for the original C&A process.

5. ACCELERATED C&A PROCESS

This section provides guidance for implementing an accelerated C&A process for Rapid Development Projects and for information systems that require an expedited accreditation decision. The accelerated C&A process shall be used on a limited basis, and the CIO must authorize, in writing, use of the abbreviated process on an individual basis. The accelerated C&A process shall only be used in the following situations:

1. New information system that is part of designated Rapid Development Project.
2. New information system is required to implement or support a critical business mission.
3. New information system that is of such great business or political significance that a quick accreditation decision turnaround is needed.
4. Threat environment changes for existing mission critical information system, but system continues to operate at acceptable level or risk.
5. Major system modifications are made to mission critical information system, but system continues to operate at acceptable level of risk.
6. System security level is increased for mission critical information system, but system continues to operate at acceptable level of risk.

The accelerated C&A process shall follow the logical flow of the full C&A process, however, the certification evaluation will involve only an internal self-assessment. Further, full authorization to operate cannot be granted through the accelerated process, because the limited certification evaluation will not generate sufficient information for the CIO/DAA to make an informed risk-based decision for long-term operation. The CIO/DAA may grant only an interim accreditation subject to operational limitations and restrictions, and a full C&A will need to be initiated within one-hundred eighty (180) days.

The tasks and sub-tasks documented in Section 4 are streamlined for the abbreviated process to ensure rapid progression through the C&A phases. The significant differences between the full C&A process and the accelerated process are primarily within the Security Certification Phase, which is normally the most resource intensive and time-consuming component of the C&A.

The following table details the differences between the full C&A process and the accelerated C&A process. All tasks and sub-tasks documented in Section 4 are listed in the left column. Differences that exist between the full C&A process and the accelerated process are detailed in the left column.

Full C&A Process		Abbreviated C&A Process
PERFORM BUSINESS RA		No difference, System Owner must perform Business RA, when appropriate.
INITIATE SSP		No difference, System Owner must develop SSP, when appropriate.
PERFORM IS RA		No difference, System Owner must perform IS RA, when appropriate.
CERTIFICATION PREPARATION		
Sub-task 1:	Verify that the information system has been fully characterized and documented in the SSP.	No difference, System Owner must review the SSP.
Sub-task 2:	Verify that the System Security Level of the information system has been correctly documented within the SSP.	No difference, System Owner must review the SSP.
Sub-task 3:	Verify that potential threats that could exploit information system flaws or weaknesses have been identified and documented within the Business RA and IS RA.	No difference, System Owner must review the Business RA and IS RA.
Sub-task 4:	Verify that the security controls implemented for the information system have been correctly identified and documented within the SSP.	No difference, System Owner must review the SSP.
Sub-task 5:	Verify that flaws or weaknesses in the information system that could be exploited by potential threats have been identified and documented within the IS RA	No difference, System Owner must review the IS RA.
Sub-task 6:	Verify that the expected residual risk to CMS operations and assets has been determined and documented within the IS RA and SSP.	No difference, System Owner must review the IS RA and Business RA.

Full C&A Process		Abbreviated C&A Process
		System Owner requests use of the accelerated C&A Process, and the CIO/DAA grants written authorization to use the Abbreviated C&A Process.
NOTIFICATION		Only the CIO/DAA, Senior Agency Information Security Official, and ISSO shall be notified that the information system will require security C&A.
RESOURCE IDENTIFICATION		
Sub-task 1:	Determine the level of effort required for the C&A of the information system.	Not required for abbreviated C&A process.
Sub-task 2:	Determine the resources required for the C&A of the information system.	Not required for abbreviated C&A process.
Sub-task 3:	Prepare and authorize a C&A project plan.	Not required for abbreviated C&A process.
SSP ANALYSIS, UPDATE, AND ACCEPTANCE		
Sub-task 1:	Analyze the SSP and IS RA to determine if the system security controls are adequate.	The System Owner, rather than the CMS C&A Evaluator, shall review the SSP to determine if any additional security controls are necessary.
Sub-task 2:	Modify system security controls based upon the results of the independent analysis and recommendations issued by the CMS C&A Evaluator, and update the SSP and IS RA.	No difference, System Owner shall implement necessary security controls and update the SSP accordingly.
Sub-task 3:	Review the SSP and IS RA to determine if the expected residual risk to CMS operations and assets is acceptable.	No difference, System Owner must review the SSP and IS RA to determine if the expected residual risk is acceptable and complies with the CIO's expectations for acceptable risk.

	Full C&A Process	Abbreviated C&A Process
SECURITY CONTROL VERIFICATION		
Sub-task 1:	Request and assemble all documentation, materials, and resources required for completion of the ST&E review.	Not required for abbreviated C&A process.
Sub-task 2:	Assemble and review previous evaluation results of the security controls implemented for the information system, and determine whether previous results are suitable for reuse.	System Owner, rather than the CMS C&A Evaluator, shall review previous evaluation results to determine whether they are suitable for reuse.
Sub-task 3:	Develop and authorize the ST&E Rules of Engagement.	Not required for abbreviated C&A process.
Sub-task 4:	Develop and authorize the ST&E Work Plan.	Not required for abbreviated C&A process.
Sub-task 5:	Perform system security test and evaluation.	The System Owner will perform an internal assessment, based upon the requirements documented within the FISCAM. In addition, the System Owner shall review prior penetration test, system test, security audit, internal assessment, review, and risk assessment documentation to identify potential vulnerabilities and weaknesses in the information system.
Sub-task 6:	Prepare the ST&E report.	The System Owner shall develop a report that details any vulnerabilities or weaknesses revealed during the self-assessment that create risk to CMS. The System Owner shall include recommendations for reducing or eliminating each vulnerability.
SECURITY CERTIFICATION DOCUMENTATION		
Sub-task 1:	Provide the System Owner with the ST&E report.	Not required for abbreviated C&A process.

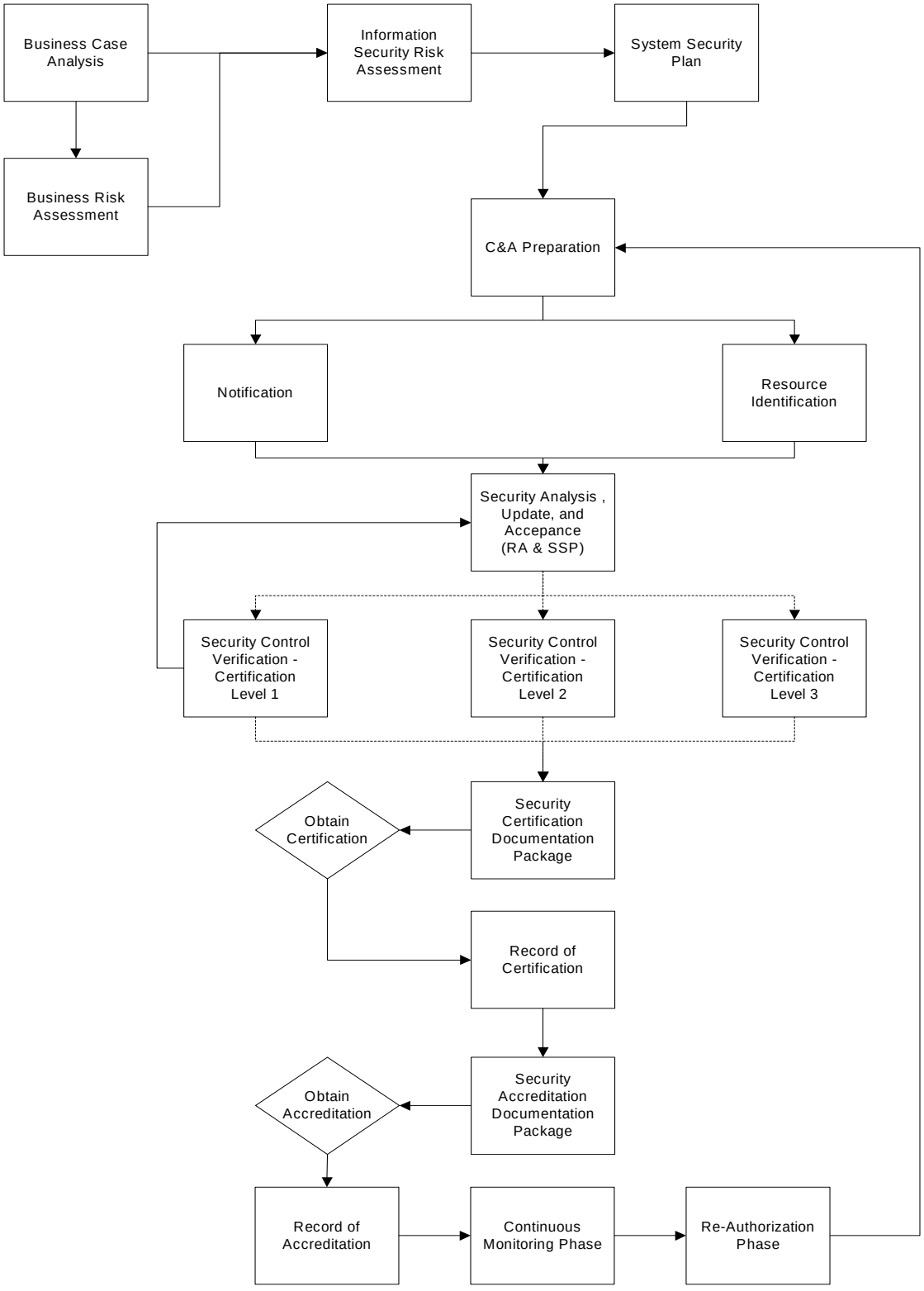
	Full C&A Process	Abbreviated C&A Process
Sub-task 2:	Develop the system CAP and update the SSP based upon the results of the ST&E, and any modifications to the security controls in the information system.	The System Owner shall develop the CAP and update the SSP based upon the results of the self-assessment, and any modifications to the security controls in the information system.
Sub-task 3:	Assemble and deliver the Security Certification Package.	The Security Certification Package will not contain the ST&E Report, but instead will contain the internal assessment results. The internal assessment results should be documented within the same format used for the full C&A process (Attachment 5). The remainder of the Security Certification Package will remain the same as the full C&A process. The System Owner shall issue an accreditation decision recommendation to the CIO/DAA, and include this within the Security Certification Package. The System Owner shall state that "time is of the essence" in the cover letter.
SECURITY ACCREDITATION DECISION		
Sub-task 1:	Review the actual residual risk to CMS operations and assets based upon the confirmed vulnerabilities in the information system, and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.	No difference.
Sub-task 2:	Determine if the actual residual risk to CMS operations and assets is acceptable.	No difference, except the CIO/DAA may grant only an interim approval to operate if the abbreviated C&A process is used. The interim approval shall be valid for one hundred eighty (180) days, during which time the full C&A process must be initiated to receive full authorization to operate the information system.

Full C&A Process		Abbreviated C&A Process
SECURITY ACCREDITATION DOCUMENTATION		
Sub-task 1:	Prepare the final Security Accreditation Package, and transmit copies of the final Security Accreditation Package to the System Owner and any other CMS officials having an interest in the security or operation of the information system.	No difference.
Sub-task 2:	Update the SSP and CAP, if necessary, based upon the final determination of actual residual risk to CMS operations and assets.	No difference.

Attachment 1 – C&A Integrated Into the CMS SDLC

C&A Phase	C&A Process	SDLC Phase
Pre-Certification	1.0 Business RA	**Business Case Analysis Acquisition**
	2.0 Develop SSP 3.0 IS RA	**Requirements Analysis Design and Engineering**
Initiation	4.0 Certification Preparation	**Development**
	5.0 C&A Notification	
	6.0 C&A Resource Identification	
	7.0 SSP Analysis, Update, and Acceptance	**Testing**
Certification	8.0 Security Control Verification	**Implementation**
	9.0 Security Certification Documentation	
Accreditation	10.0 Security Accreditation Decision	
	11.0 Security Accreditation Documentation	
Continuous Monitoring	12.0 Configuration Management and Control	**Operations and Maintenance**
	13.0 On-going Security Control Verification	
	14.0 Status Reporting and Documentation	
Re-authorization	15.0 Re-authorization	

Attachment 2 – C&A Process Flow



Attachment 3 – Standard Rules of Engagement

1. Background and Statement of Purpose

A critical component of the CMS IS program is the Security Certification and Accreditation (C&A) process. Security certification of information systems is performed to verify that proper security controls are implemented, in accordance with legal, regulatory, and policy requirements. The Security Testing and Evaluation (ST&E) process is conducted to assess the management, operational and technical controls. The entity performing the security testing is referred to as the CMS C&A Evaluator.

The Rules of Engagement governing the ST&E process are established within this document. These Rules of Engagement define the scope of the ST&E process, the testing period, the types of testing that will be performed, and management requirements.

2. Administrative

2.1 Time-frame

Certification testing is scheduled to begin on [*date*]. It is expected that the ST&E process will be completed by [*date*]. All testing activities shall be conducted during standard business hours; between 8:30 AM and 5:00 PM. If the CMS C&A Evaluator requires testing to be conducted beyond these hours, management authorization must be obtained.

The schedule for testing shall be provided, and the timeline for each site visit shall be completed in the CMS Penetration Test Site Schedule. CMS will contact each site to verify that the time set forth will be acceptable to all parties.

2.2 Points of Contact

Government Task Leader (GTL) or Project Leader

Name	
Title	
Name of Organization	
Address	
Address Line 2	
City, State, Zip Code	
E-mail Address	
Telephone Number	

CMS C&A Evaluator

Name	
Title	
Name of Organization	
Address	
Address Line 2	

City, State, Zip Code	
E-mail Address	
Telephone Number	

System Owner

Name	
Title	
Name of Organization	
Address	
Address Line 2	
City, State, Zip Code	
E-mail Address	
Telephone Number	

System Maintainers

Name	
Title	
Name of Organization	
Address	
Address Line 2	
City, State, Zip Code	
E-mail Address	
Telephone Number	

Information System Security Officer

Name	
Title	
Name of Organization	
Address	
Address Line 2	
City, State, Zip Code	
E-mail Address	
Telephone Number	

2.3 Resource Requirements

The CMS C&A Evaluator shall provide qualified security testing personnel, equipment, and materials necessary to complete the ST&E procedures. The CMS C&A Evaluator's key personnel shall have suitable past experience in conducting ST&E assessments, and must have knowledge of CMS security policies, standards, guidelines, and procedures.

To promote the efficient and proper completion of the ST&E process, the CMS C&A Evaluator will require that technical staff responsible for the regular management and administration of *[system name]* to be made available during the ST&E process. Technical staff shall be readily available to answer questions of technical nature, and to resolve any problems or difficulties the CMS C&A Evaluator may encounter.

All security documentation, including the Business RA Report, the SSP, the System RA Report, any local security policies and Standard Operating Procedures, the Disaster Recovery Plan, the Business Continuity Plan, and a current network diagram shall be provided to the CMS C&A Evaluator. The technical staff, on completion of the testing, shall provide to the CMS C&A Evaluator the Intrusion Detection System (IDS) results or a statement attesting to the IDS log file findings for analysis. In addition the technical staff shall provide the incident handling procedures to the CMS C&A Evaluator to determine the handling of a suspect incident if identified by the IDS.

2.4 Security Requirements

The CMS C&A Evaluator shall comply with the information systems security requirements set forth in these Rules of Engagement, in the CMS Policy for Information Security, the CMS Information Security Handbook, and all local security policies not in direct conflict with CMS security requirements. CMS policy takes precedence over local security policies.

2.4.1 Personnel Security

All non-governmental employees of the CMS C&A Evaluator shall meet personnel security / suitability standards commensurate with their position sensitivity level, and are subject to personnel investigation requirements. Access to government information shall be granted upon demonstration of a valid need to know, and not merely based upon position, title, level of investigation, or position sensitivity level. All non-governmental employees of the CMS C&A Evaluator are required to complete the proper security requirements, in accordance with the CMS and DHHS Personnel Security / Suitability Handbook. All CMS C&A Evaluator personnel who will be responsible for technical analysis of information systems are required to obtain a Level 5 Moderate Risk or Level 6 High Risk security clearance.

2.4.2 Handling and Storing Sensitive Information

The CMS C&A Evaluator is required to handle, store, disseminate, and dispose of any sensitive CMS information collected, shared, or developed during the ST&E process, in a manner consistent with CMS security policy. Sensitive information may be shared only with individuals on a need-to-know basis. Proper security practices must be followed to prevent accidental or intentional disclosure of sensitive information.

On completion of testing, all materials collected or shared during the ST&E process, in either electronic or hard copy format, must be disposed of securely. Hard copy documents must be either returned to CMS or shredded, and all electronic data must be purged.

3. Scope of Testing

3.1 System Environment

[*Define technical boundaries for certification task here*]

3.2 Test Procedures

The CMS C&A Evaluator shall:

- Schedule and conduct security testing, collaborating with CMS employees and the System Owner as necessary.
- Provide a ST&E Work Plan that identifies the objective of each test, pre-requisites that must be completed prior to the test, all test procedures that will be conducted, and expected results.
- Conduct only those test procedures that have been mutually authorized by the CMS GTL and the System Owner.
- Notify the CMS GTL and technical personnel prior to performing any testing. All tests shall be done with the full knowledge and authorization of CMS.
- Permit CMS, the System Owner, or technical personnel to monitor and observe test procedures.
- Cease immediately all testing activities at the direction of the CMS GTL, or the System Owner, or technical personnel.
- Notify CMS and the System Owner of all software, programs, applications, utilities, scripts, and other forms of tools that will be used to complete the security testing. No such tools shall be used without the express authorization of CMS and the System Owner.
- Follow generally accepted industry and government testing standards.
- Perform all testing in a non-destructive, least intrusive manner. No Denial-of-Service test procedures, or any other test procedures with the potential to cause widespread damage or disruption shall be performed.
- Maintain a test log and document all results.
- Verify the authenticity and validity of actual test results.
- Inform immediately the CMS GTL and the System Owner if a serious vulnerability or defect is discovered, which poses an imminent danger to the system or network environment.
- Obtain mutual authorization from the CMS GTL and the System Owner if it becomes necessary to modify or vary from any of the agreed-upon test procedures.
- Be able and available to reproduce any test result at the request of CMS or the Business Owner.
-

4. Work Product

The CMS C&A Evaluator shall record all test results within the ST&E Work Plan and within a test log. After completing the certification evaluation, the CMS C&A Evaluator shall produce a Security Test and Evaluation (ST&E) Report, which will form part of the Certification Package to be delivered to the CIO/DAA. The test findings shall be documented in the ST&E Report after the onsite and offsite testing has been completed. The ST&E Report shall be made available to the CMS GTL and the System Owner for review, prior to final assembly of the Security Certification Package.

5. ST&E Impact Statements

It is CMS' intent to conduct the ST&E tests with minimal impact upon the infrastructures that manage / own the systems. In an effort to accommodate the concerns of the System Owner, CMS realizes that tests conducted on systems / networks may sometimes incur some degradation of bandwidth or system performance. In these cases, the CMS C&A Evaluator may be asked to conduct the tests after the business hours, during the week or over the weekend to avoid

impacting the users / customers during regular business hours (8 a.m. thru 5 p.m., local time). The schedule of testing is to be determined before the visit and agreed upon by the CMS GTL, System Owner and CMS C&A Evaluator management.

The CMS C&A Evaluator will not utilize any "Denial-of-Service" attack techniques as part of the penetration testing. All penetration activities will be controlled to minimize impacts on operational systems.

In the unlikely event of an adverse effect on the underlying network, operating system, application or hardware, the CMS C&A Evaluators will adhere to a strict protocol to minimize the impact on mission critical operations:

- Prior to any testing, emergency contact information will be given to all individuals authorized to halt the tests.
- Upon request of the Contractor or CMS GTL, the CMS C&A Evaluator will halt the current phase of testing, immediately, and proceed with the next phase of tests.
  - Should the Contractor (Data Center or CMS Partner) request a halt to the current phase of testing, the Contractor will contact the on-site CMS representative, CMS GTL (Susan Szamski @ 410-786-3020) or CMS GTL Backup (Maria McMahon @ 410-786-3023) with the supporting evidence of degradation.
    - Contingency contact: 410-786-1890
  - Once the current phase of testing has been halted, the CMS C&A Evaluator will report to the CMS C&A Evaluator Project Leader who will then inform the CMS GTL of the interruption of testing and provide any information in regards to the nature of the tests conducted at the time of the request.
- The CMS representative will have the responsibility to research the issue and advise the CMS GTL or CMS GTL Backup of the details of the problem.
- The CMS GTL will then direct the CMS C&A Evaluator as to the next course of action:
  - Resume the interrupted phase of testing;
  - Research and investigate the nature of the degradation with the intent to resume the phase of testing after determining measures that will prevent further degradation;
  - Resume the interrupted phase of testing during non-business hours as agreed upon by the CMS GTL, Contractor and the CMS C&A Evaluator;
  - Continue with the new phase of testing; or
  - Cease all testing.

Attachment 4 – ST&E Work Plan Template

1.1. TITLE		
Summary results		**Pass** ☐ **Fail** ☐ **N/A** ☐
Objective		
Pre-requisites		
Test Steps	**Expected Results by System Security Level**	**Actual Results**
	☐ High Expected High Security result. ☐ Moderate Expected High Security result. ☐ Low Expected High Security result.	N/A ☐ Meets ☐ High ☐ Moderate ☐ Low ☐ None
Comments / Further Information Required:		
Post Test Activities:		

The testing signified by this examination has been completed in partial fulfillment of the requirements for Certification and Accreditation for [*CMS system*].

The results are accurate as submitted.

Signatures

_____ _____

[*Tester*] Date

_____ _____

[*Witness*] Date

Attachment 5 – ST&E Business Risk Template

3.4.1 Business Risk:	[Click here and enter Title]

NIST CVE #:

Priority: (Priorities can be High Risk, Moderate Risk, Low Risk)

[Click here and enter High Risk, Medium Risk, or Low Risk]

Ease of Fix: (Ease of Fix can be Easy, Moderately Difficult, Very Difficult, No Known Fix)

[Click here and enter Easy, Moderately Difficult, Very Difficult, or No Known Fix]

Estimated Work Effort: (Estimated Work Effort Can be Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

[Click here and enter Minimal, Moderate, Substantial, or Unknown]

Description:

[Click here and type detailed description of the business risk]

Suggested Remediation:

1. [Click here and type the recommended fix]

Status:

[Click here and type the business risk status]

Attachment 6 – Sample Security Certification Package Cover Letter

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-15
Baltimore, Maryland 21244-1850

[*Department/Organization*]

TO:

FROM:

SUBJECT:

The [*CMS C&A Evaluator*] has completed the certification evaluation of [*system name*]. A security accreditation decision for [*system name*] is requested by [*date*]. The attached Security Certification Package provides current and accurate information to enable you to reach an informed, risk-based accreditation decision.

Please find within the attached Security Certification Package a copy of the security certification form, the [*system name*] SSP, the CAP, and the Security Test and Evaluation Report prepared by [*CMS C&A Evaluator*]. The [*CMS C&A Evaluator*] and I are available to discuss any questions regarding the CMS C&A Methodology and the certification evaluation. Please contact [*name*] of [*organization*] at [*phone number*] if you require a meeting.

Sincerely,

[*System Owner*]

Attachment

cc: Director, SSG

Attachment 7 – CMS Security Certification Form

	Certification is required for the following reason(s):
	New System
	Major system modification
	Increased system data sensitivity level
	Serious security violation
	Changes in the threat environment
	Expired Accreditation

The signatures below attest that the appropriate technical certification evaluations have been conducted successfully.

_____

Name of System

_____

CMS Component

(*printed name*)_____(signature)_____
CMS Component Information System Security Officer (ISSO) **Date**

I, the System Owner / Manager / Maintainer, have examined the controls implemented for this system and consider them adequate to meet agency policy and the relevant business requirements. I also understand and accept the risk inherent in processing on a network or at the installation(s) that supports this system, particularly where the support system is operated outside of my management control. This certification is based on the documented results of the design reviews, system test and the recommendations of the testing teams.

(printed name)_____(signature)_____
System Owner / Manager **Date**

(printed name)_____(signature)_____
System Maintainer (Manager) **Date**

Certification Restrictions

Certification is granted with the following restrictions (use additional pages if necessary):

Certification Actions

The following specific actions are to be completed by the dates indicated (use additional pages if necessary):

Attachment 8 – Sample Accreditation Decision Recommendation

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-15
Baltimore, Maryland 21244-1850

[*Department/Organization*]

TO: [*CIO/DAA*]

FROM: [*CMS C&A Evaluator*]

SUBJECT: Security Accreditation Decision Recommendation

[*CMS C&A Evaluator*] has completed its security certification review of the [*system name*]. During the certification evaluation [*number*] high-risk and [*number*] moderate-risk vulnerabilities were identified. Recommendations for corrective actions that will reduce or eliminate each vulnerability have been issued to the System Owner, and most corrective actions may be implemented within minimal time and resource commitment. Conditioned upon proper implementation of the recommended corrective actions, as detailed in the Corrective Action Plan, [*CMS C&A Evaluator*] considers the security controls implemented to protect the [*system name*] sufficient to meet current CMS system security requirements. [*CMS C&A Evaluator*] recommends that full authorization to operate [*system name*] be granted.

[*CMS C&A Evaluator*] is available to discuss any questions regarding the review. Please contact [*Government Task Lead*] of [*organization*] at [*telephone number*] if you require a meeting.

Sincerely,

[*CMS C&A Evaluator*]

Attachment

cc: [*Government Task Lead*], [*System Owner*]

Attachment 9 – Sample Security Accreditation Decision Letter

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-15
Baltimore, Maryland 21244-1850

[*Department/Organization*]

TO:

FROM:

SUBJECT:

The Systems Security Group (SSG) has completed its review of the [*system name*]. The security controls implemented to protect the [*system name*] are considered sufficient to meet the current system security requirements and an accreditation has been granted.

There are actions that must be addressed by the system owner / manager prior to the Accreditation expiration date of [*date*]. The items are described in the attached System Accreditation Form. As the system owner / manager, you must address these items and resubmit the SSP prior to [*date*] to allow for re-accreditation processing.

In addition, each MA's system owner shall review the certification documentation (i.e. RA, SSP, and system test documentation) annually; update the documentation where necessary to reflect any changes to the system; and submit a copy of updated information to the Chief Information Officer (CIO) or Designated Approving Authority (DAA).

SSG is available to discuss any questions regarding the CMS C&A Methodology and the certification review. Please contact [*Government Task Lead*] of [*organization*] at [*telephone number*] if you require a meeting.

Sincerely,

Chief Information Officer &
Director, Office of Information Services

Attachment

cc: Director, SSG

Attachment 10 – CMS Security Accreditation Form

Accreditation
Interim Accreditation

	Accreditation is required for the following reason(s):
	New System
	Legacy System
	Major system modification
	Increased system security level
	Serious security violation
	Changes in the threat environment
	Expired Accreditation

I have examined the controls implemented for **[*System Name*]** and consider them adequate to meet agency policy and the system appears to be operating at an acceptable level of risk.

A

The signature below attests to the formal management approval to process (system accreditation) based on the conditions listed in attachments B and C for the system listed above. This approval to process expires at the close of business, on the following date: **[*Date*]**.

_____
(signature) (date)

[*Chief Information Officer*]
Chief Information Officer &
Director, Office of Information Services

B TAB B: Accreditation Restrictions

Accreditation is granted with the following restrictions (enter NONE if no restrictions):

None

(add additional rows / page(s) if necessary)

C TAB C: Accreditation Actions

Failure to meet the assigned due dates without prior approval invalidates this accreditation. The following specific actions are to be completed by the date(s) indicated (enter NONE if no actions):

Control / Action Description	Due Date

(add additional rows / page(s) if necessary)

End of Document